PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04L 9/06	A1	WO 98/05142
		(43) International Publication Date: 5 February 1998 (05.02.98)

(21) International Application Number: PCT/EP97/04062

(22) International Filing Date: 25 July 1997 (25.07.97)

(30) Priority Data:
196 30 354.0 26 July 1996 (26.07.96) DE
97102436.9 14 February 1997 (14.02.97) EP
(34) Countries for which the regional or international application was filed: AT et al.

(60) Parent Application or Grant
(63) Related by Continuation
US 08/807,572 (CIP)
Filed on 27 February 1997 (27.02.97)

(71)(72) Applicant and Inventor: SCHNOOR, Ernst, Erich [DE/DE]; Alois-Wohlmuth-Strasse 25, D-81545 München (DE).

(74) Agent: LEONHARD, Reimund; Leonhard, Olgemöller, Fricke, Josephspitalstrasse 7, D-80331 München (DE).

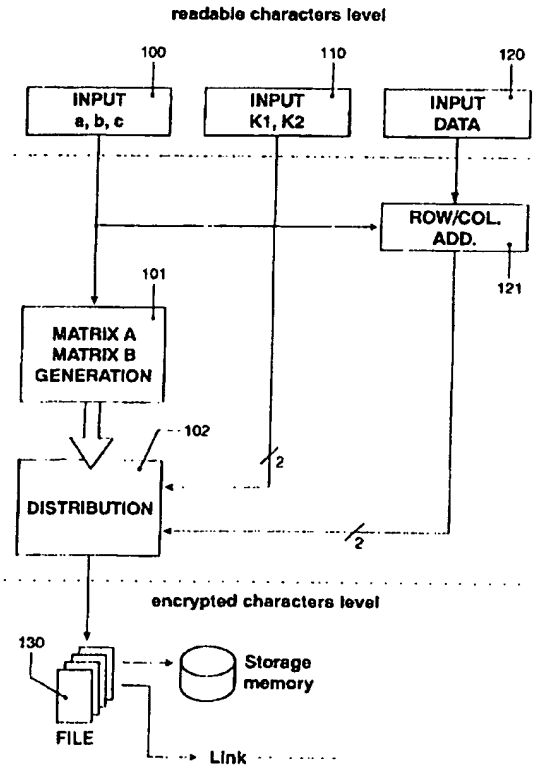
(81) Designated States: CA, GB, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: MULTI MATRIX ENCRYPTION FOR PRIVATE TRANSMISSION OF DATA

(57) Abstract

The technical field of the invention concerns methods for the encryption of data to be safely transmitted within electronic networks. The invention also concerns a device in chip form for executing the aforementioned method. The chip may be designed to encrypt the text (at the sender's end). It may according to the invention also be designed to decrypt encrypted data (at the receiver's end). Suggested are the steps of providing at least one field input in a coding step to define at least a first array or matrix with distributed ASCII elements, which ASCII elements are filling said matrix or array purposeful and unique, but in a distributed manner; said input data is transformed via a transformation to at least a first and a second index, uniquely addressing said at least one array or matrix in order to determine encrypted characters.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Multi matrix encryption for private transmission of data

The technical field of the invention concerns methods for the encryption of data to be safely transmitted within electronic networks[1]. The invention also concerns a device in chip form for executing the aforementioned method. The chip may be designed to encrypt the text (at the sender's end). It may according to the invention also be designed to decrypt encrypted data (at the receiver's end).

Encryption programs are in public domain for a long time; their spreading grows due to the evolutional expanding of networks. Many encryption processes call themself "safe" or "private", but use a vast amount of processing software and hardware.

The **object of the invention** is such that security is achieved with little effort and easy handling by an easy-to-cope-with processor performance, even though the transmission of the encrypted (encoded) files itself is simple.

The invention uses an n-dimensional matrix (e.g., two-dimensional: 10 x 10 lines and columns [decimal number system], 16 x 16 lines and columns [hexadecimal number system], up to 64 x 64 lines and columns [number system 64] and even higher, in which matrix a specific quantity of ASCII characters is contained in an irregularly distributed manner. The specific quantity may be some ASCII characters (matrix 10 x 10 to matrix 15 x 15), all ASCII characters (matrix 16 x 16) or character combinations, the available elements of which reach beyond the number of single ASCII characters (matrix higher than 16 x 16).

The distribution of the elements in the matrix is depending on a user's inputs as a variable generation of keys. For instance, when encrypting via a two-dimensional matrix, every individual ASCII character of the (unciphered or "plain") input data stream or file is transformed to a four-digit number which is then split up into two two-digit numbers. The digits of the two new

[1] As far as the United States are concerned (US designation), this is a continuation-in-part application of 08/807,572 of February 27, 1997 filed as national application.

numbers form the indices or indexes for a respective row and column of the irregularly distributed quantity of the ASCII characters in the respective matrix to read out two ciphered characters. The sequence of these ciphered characters selected from the "distributed matrices" according to said indexes forms the encrypted text, designated for private data transmittal.

The factors of the transformation are depending on the user inputs as variable generation of keys. Changing even one character during the user input will thus result in a completely different distribution of characters in the matrix.

The invention employs a pseudo-random **free** sequence of digits (claim 13), being predetermined and almost independently obtained at both ends of the transmittal chain, just the type or the analytical function and the user key (input or fixum) is used. Thus, the sequence may be generated independently at both ends. The sequence is then employed (used) or further processed for encrypting.

The method is inverted (or reversed) for the decryption (deciphering). The four-digit number is derived from the two characters of the encrypted file or data stream and the indices of their arrangement in the respective matrix. The transformation in reverse order will then result in the ASCII character of the recovered input data file or stream, after "private transmission" via a link has taken place.

As a result of the matrix generation and the irregular distribution of the characters there is an interruption in the direct correlation between input characters and encrypted output characters. Therefore, it will hardly be possible to derive the input from the characters of the encrypted file or stream with the help of characteristics and distinguishing features of the language used.

A thought shall be addressed to the way of how the **distributed ASCII elements** are obtained in said at least one matrix.

Starting from the user input, all field inputs are taken together and then represented for example in decimal representation. To reduce the occurences of "1" and "2", three digit decimal representations can be truncated to only remain the two lower significant digits. Instead of employing a random or pseudo-random sequence, the invention uses known functions, such as cosine, sinus, logarithm or other functions to use their result as a long irregular but reproducible sequence of digits when a certain argument is given to these functions. The argument is taken from the aforementioned consecutive decimal representations with truncated "1" and "2". Which functions are used, can be agreed between sender and transmitter, but by defining the function by its type, the long reproducible but irregular sequence is defined at both ends. More than one function can be agreed, and linear transformations of functions can also be agreed (2xcos, 1/2xcos or 4+cos or similar). The argument for each function is taken as a section of the consecutive decimal representation, for instance with 1 to 18 digits. The result of the function, calculated with the argument is said reproducible sequence which should have at least 10 digits behind the comma. These digits can be consecutively rowed with each function agreed. For example, 8 functions are agreed and 10 digits behind the comma are used from the function (applied to the argument), thus a block of 80 digits is obtained. This can be done a couple of times, for instance four times, to achieve 4x80 long irregular, but reproducible sequences of digits which can easily be obtained at the other end of the transmittal chain as well.

The sequences can now be used to obtain a matrix (array) with distributed ASCII elements by reduction-filtering said sequences to a reduced sequence which has each digit occuring only once. If, for example, the reduction-filtering is to achieve a 10 digit sequence, all digits "1" to "9" occur once, but freely distributed. One example is to scan the 80 mentioned digits and take a digit only into the reduced-filtered sequence, if it is not prior occured. For each matrix to be obtained, this can be performed corresponding to the amount of digits available in the

respectively selected digit system (10, 16, 60 or similar). The array (matrix) with distributed ASCII elements which are filling said matrix purposefully and uniquely is obtained by swapping rows and columns according to the reduction-filtered sequence. A number of operations of swapping alternatively columns and rows proceed before the finally distributed matrix for encrypting the text is obtained. More than one matrix can be used to enhance the private transmission of data; a compromise between complexity and safety is the use of two encrypting arrays (matrixes) with freely distributed ASCII elements.

If claims refer to only one prior claim, this is to be understood to refer back to all preceeding claims.

The invention will be described by way of embodiments.

Figure 1 is a first embodiment of a software implementation according to the invention.

Figure 2 is a second block diagram represented embodiment of a hardware implementation according to the invention in a device delivered as chip.

Figure 3a,
Figure 3b are examples of two matrices or arrays A and B having distributed ASCII characters according to the distribution and matrix filling step according to the invention.

Figure 4a,
Figure 4b are examples of larger matrices or arrays having a dimension of 2 and 15 columns and 15 rows each, filled with almost the full 8-bit character set of a standard ASCII code in distributed manner.

Figure 4c is a standard ASCII table having no "distribution" according to the invention, but a "regular order of sequence".

Figure 5a,
Figure 5b are two similar matrices according to Figure 3a and 3b achieved with the embodiments of Figure 1 or Figure 2 of the invention, but with a different key input than the matrices of A and B of Figure 3a and 3b.

Figure 5c is an irregular sequence of digits, e. g. generated from the natural logarithm, used for indexing the arrays.

Figure 5d is the distribution of Figure 5c and its irregular sequence of digits cleared for double numbers (digits) to fill up the rows and columns of a matrix or array or to irregularly distribute regular organized ASCII characters to form a distributed array.

Figure 6 is an example of a file having 50 "e" characters in a continuous stream of input data.

Figure 7 is a two-page picture of what is achieved as output file when using the e-file of Figure 6 with an encryption process according to the invention having 10 x 10 matrices A and B and using a certain three-key data input to define the encryption process according to the invention.

Before the figures are described in greater detail, the language of the description and the terms used herein are to be defined more closely.

The method may be implemented as a sequence of program steps or in hardware implementation with micro sequencing. The software can be performed in any current program language (BASIC, PASCAL, C++, UNIX, and others). Assemblers for hardware may be utilized.

Meaning of terms used in the description:

Message:
Sequence of data transmitted on electronic channels or links.

Sender:
Sender of a message who encrypts the plaintext of the message.

Addressee:
The receiver of a message who, in turn, decrypts the message.

ASCII:
American Standard Code for Information Interchange.

ASCII character:
The character that can be represented on acomputer according to the ASCII code. It may as well represent a pixel or part of a longer pixel.

ASCII digits:
The numbers which are allocated to the ASCII characters in the order system of the ASCII code (hexadecimal: 00 to FF, decimal: 0 to 255, binary: 0000 0000 to 1111 1111).

Encryption:
The transformation of input data that can be represented on computers to a sequence of picture or ASCII characters or an executable file.

Decryption:
The transformation of the encrypted text (ASCII characters) to plaintext which can be represented on computers.

Key data:
The respective user inputs (sender and addressee) for encrypting the plaintext and for decrypting the encoded text as variable generation of keys.

Distribution matrix:
An irregular distribution of ASCII characters, systematically arranged in n-dimensions. In doing so, the number (n) of dimensions in practical application may be 2 (10 x 10 to 64 x 64 characters) up to 8 (2x2x2x2x2x2x2x2 characters).

Number system:
Systematic arrangement of numbers in the region to base 2, theoretically up to base (infinite-1). In practical application from base 2 to base 64.

Transformation:
The transformation of figures of an ASCII character (two-digit) to a number from which the indices for the n-dimensional matrix may be derived.

The method comprises in one embodiment the following program steps, as can be seen from Figure 1.

1. Up to three key data words a, b, c will be given in step 100, up to a total length of 36 characters (for instance, the data in square brackets). They can be typed in by a keyboard KBD as shown in Figure 2, they can as well be fixed parameters in a en-/decryption device, not to be altered by the user, but the manufacturer.

   Input a: PIN (personal identification number) with 4 figures, e. g. [1234]

   Input b: Bank account number with up to 16 characters or any other identifier of the sender with arbitrary blanks, according to his choice, e. g. [9876-543-ABC]

   Input c: Password with up to 16 characters (with arbitrary blanks), e. g. [Mount Everest]

2. Two internal check values K1, K2 may additionally be given in step 110 or may be generated from the key data which are used for identification of the sender and for checking the inputs a, b and c at the addressee's end. These check values will be incorporated in the message to be encrypted.

3. From the key data of input a (PIN) and the ASCII figures of the entered data b and c the method will calculate a first irregular sequence of the numbers from 0 to 9 (or from 0 up to the highest number of the respectively used number system). The irregular sequence may e. g. be generated from the logarithm to the base of 10 (common logarithm), the natural logarithm (base e), the logarithm to the base of 2, the square root, sine, cosine, tangent, arc tangent or the comparable mathematical operations with at least 10 places behind the decimal point. A

respectively longer irregular sequence is determined for higher number systems. An example of such sequence may be seen from Figure 5c. The length may be adapted to the size of the matrices to be used for encryption:

Matrix 10x10; e. g. [0961742538]
Matrix 16x16; e. g. [0ADBE96174253F8C]

4. A second irregular sequence will be generated according to the same principle but with a changed starting point. Examples are given below:

Matrix 10x10; e. g. [6741289503]
Matrix 16x16; e. g. [6D7C41A289FE50B3]

5. First and second sequence will be combined in step 101 to form one matrix to the extent of the respectively used number system (matrix A), i. e., in such a way that there will be in toto an irregular but complete distribution of all elements of the matrix in all lines and columns of the matrix (this is called the filled distribution matrix).

6. A second matrix (matrix B) will be generated similar to step 101 and according to the same principle but with changed starting point (third sequence and fourth sequence), again with a complete, but different, distribution of all elements of the matrix in step 102.

7. A part of the or all ASCII characters may be used as elements of the respective matrix up to a length of 16 lines and 16 columns; other characters will have to be selected beyond that. In this embodiment, the combination of two each letters or ASCII characters is implemented.

8. For encryption, the respective ASCII number (digit) of the input data, to be encrypted, is consecutively transformed to a four-digit number ABCD (decimal: between 0000 and 9999) in steps 120 and 121. A multiplicity of operations

and combinations may form the transformation (addition, subtraction, multiplication, division, shifting of bits). The transformed number should not fall below the value 0000 and should not exceed the value 9999 (decimal), EEEE (15x15) in the number system to the base of 15, JJJJ (20x20) in the number system to the base of 20 and ZZZZ (36x36) in the number system to the base of 36).

9. The four-digit number ABCD is then split up into two halves (AB -> 'ab' and CD -> 'cd'). For the created two new numbers (ab) and (cd), in the decimal number system in the value range from 00 to 99 each, the respective pertinent ASCII character is alternately indexed for in Matrix A and Matrix B (lines 0 to 9 for a,c and columns 0 to 9 for b,d) and linked to form the encrypted file or data stream in step 130.

With higher number systems there is an appropriately larger value range for the two-digit number. Since two encrypted characters are created due to the splitting up of the four-digit number into two halves, the encrypted data is double the length of the initial input data. With number systems higher than hexadecimal (16x16), which require at least two-digit characters for the necessary quantity of elements in the matrix, the coded data is four times longer than the input data.

10. For securing integrity and authenticity of the message to be transmitted the method may in a further embodiment determine a check value K3 as sum of all ASCII characters of the plaintext and will incorporate this check value in the message to be encrypted according to step 110.

For decryption, program steps (1) to (7) as above will first be performed in the same manner as for encryption.

Program steps (8) and (9) will be performed in reverse order. In doing this the respective indices (line and column) will be

established in the appropriate matrix if there is a conformity between the transmitted coded character and the corresponding character in Matrix A or Matrix B and the found two digits each will again be combined to form the four-digit number.

The initial number is then determined from the four-digit number by reverse transformation of step (8). From that, the pertinent plaintext ASCII character searched for in the plaintext matrix.

The sequence of decryption will first of all, decrypt the data containing the check values K1 and K2 to compare them with the addressee's inputs a, b and c. If there is a conformity, the decryption of the data stream or file will continue.

For checking integrity and authenticity of the message the sum of all deciphered ASCII characters will be determined and compared with the transmitted and deciphered check value K3 in the further embodiment as mentioned in step (10). The decrypted plaintext or clear picture will only be released for readable representation if there is a conformity.

The steps described before can be used in either a software solution according to Figure 1 or in a hardware solution implemented in a chip, custom-made or programmed on a single chip computer. The program according to Figure 1 will then be implemented in micro-sequencing in the control 30 of Figure 2 and the two arrays A and B of Figure 1 will be contained in RAMs 10 and 11 of Figure 2. The program already explained may be used in the embodiment of Figure 2, showing a block diagram of an exemplary DIL-chip 90. For larger structures or bus systems LCC chips may be used.

In a first input step 100, the key data is given by the user, to define the distribution of the elements in the matrices A and B in step 101. The input 100 can also be a fixed input if the chip according to Figure 2 is a pre-programmed chip having a fixed key data as supplied by the manufacturer. From the key input 100, not only the distribution 102 according to the

generation step 101 are performed, but also the input data to be encrypted, as supplied in step 120, are transformed to a first and second index in step 121 to address the array in step 102. In this embodiment, the same key input is used to supply both encryption steps, the distribution 101 and 102 of the matrices and the row/column indexing or addressing in step 121.

In a further embodiment, the internal check values K1,K2 in step 110 may also be generated by the key input 100, the latter check values may in a further embodiment however also be supplied separately.

The output encrypted text from the indexing step 121 as selected from the central matrix with their distributed elements will after step 102 be stored in a file, which can be transferred via a link or can be stored on a disc or other memory device. This is the encrypted characters level, whereas the input level in steps 100,110,120 are the readable characters and thus the readable level.

It is to be self-understood that "characters" is not to only mean written characters, they may also be picture characters to define pixels or parts of pixels of video pictures.

The hardware implementation employs in one embodiment of Figure 2 the process as described in **Figure 1**. The two RAM areas 10 and 11 define in a certain place of the chip 90 the areas where the distributed elements according to step 101 and 102 are placed. The distribution is controlled by control means 30 via the address bus to address the RAMs, and when addressing a certain RAM 10 or 11 the data on the data bus will carry the character to be stored in a certain place of this RAM. The data bus DATA and the address bus ADDRESS are further used to transfer the key values from the keyboard 60 via the interface 40, when the interrupt along the interrupt or control bus CC interrupts the control 30 to indicate that key values are now present. Instead of the input of key values, a fixed value key can be placed in a certain ROM area of the chip or can be

implemented in other programmable fashion easily accessible by the manufacturer, but difficult to alter by the customer or user. The chip then bears a number or a couple of keywords to be delivered on demand along the control bus CC from the control means unit 30 and via the data bus.

An output driving unit 70 supplies the encrypted character as taken from the distributed ASCII characters in RAM 1 and RAM 2.

The chip implementation of **Figure 2** may be by program inversed to be operated as a de-encrypting device, when having the input driver 71, providing the encrypted characters to the data bus, as shown in phantom. This device operates according to the steps described before as decryption process and the skilled man will be in the position to build the decryption chip from the information given above.

Figure 3a to Figure 4b are examples of distributed matrices or arrays as they may be stored in RAM areas 10 or 11 according to **Figure 2** or in steps 101 and 102 according to **Figure 1**. Matrix A in Figure 4a shows 225 ASCII characters uniquely distributed - no value appears twice - but freely arranged according to the key inputs. The matrix A has less than 256 ASCII values, due to 31 ASCII values are used as control characters and cannot be represented pictographically.

Figure 5a and 5b show 10x10 matrices, as can also be used in RAM areas 10 and 11 of **Figure 2**. The distribution works along a sequencing step, and the control unit 30 operates along the character string or digit line of Figure 5c and takes one character at a time to define the next character to be placed in the RAM area 10 or to define the indexing addresses of an input character to be encrypted.

The irregular distribution of the ASCII characters in e.g. matrix A will be explained by the help of **Figures 5a, 5c and 5d,** using an analytic mathematical function, e.g. the logarithm and a key data value, as provided by the user in step 100 as input

variable a, b or c. Using the key input variable the logarithm will provide a digit sequence, which is no pseudo random sequence of digits. The inventive sequence having each digit more than one time. The distribution of digits seems irregular, but can be reproduced at the other end (the receiver's end) by employing the same analytical function, e.g. the logarithm, and the same key input value "a", as for example communicated between receiver and sender. It is a predetermined digit sequence (numbers 0 ... 9), depending on the user keys and the chosen analytical function.

Basing the irregular sequence of **Figure 5c**, which actually gives two sequences for different arguments of the same analytical function, the invention operates in one embodiment to select the digits one by one and to clear the sequences of Figure 5c into a digit sequence of **Figure 5d** where no digit appears twice. The first digits may illustrate this embodiment, the digits "13694" of the first line in Figure 5c are transferred 1:1 into the first sequence of digits in Figure 5d. Then another digit "4" appears in Figure 5c, which would be a dual use of the digit "4" and therefore it is deleted from the sequence of digits in the first line of Figure 5c. The next digit used for Figure 5d sequencing is the digit "5", which has the place 39 in the first line of Figure 5c. The position 39 and the further positions to select digits from the first line of Figure 5c may be fixed positions as defined by internal program or by programmed devices. Each time the next place has a digit, which already appeared, the next but one position in the digit sequence is checked. The shown examples of positions 1, 2, 3, 4, 5, 39, ... is a mere example of any positions of digits to be programmed.

A similar position oriented selection of digits in the sequence of digits is used for the second line of Figure 5c, for illustration purposes the first nine digits have been taken immediately and the eighteenth place of digits was used for the tenth digit in the second line of Figure 5d.

The sequence of Figure 5d may according to one embodiment used

for distributing the regularly arranged ASCII characters in standard sequence according to the ASCII code into ten lines and ten columns filled up with digits according to Figure 5d, where in each row there is no dual appearance of the digits 0 to 9. Having provided such a control matrix for distribution purposes it is one of multiply possible distribution rules, to exchange the positions of a regularly arranged ASCII code in a regularly arranged matrix with rows and columns along the dual digit free lines. A few characters will be explained. The left upper character of the ASCII code would stay at its place, since a "1" is mentioned in Figure 5d. The ASCII character right hand to the "1" encounters a "3", it would be placed at the third position in the row. The third position would be placed at the sixth position, the fourth position would be placed at the ninth position, each time in the same row. Such happens for each row. This is one step of distributing, many steps of distributing may be chained one to each other, they may also be organized in column fashion, which can be easily understood when transferring the row fashion as described in vertical arrangement.

Having distributed the ASCII code from regular or standard fashion by one or more, preferrably a multiplicity of such distributing operations, the matrix A appears as the control matrix for encrypting an input data to an encrypted output data file 130.

According to the invention at both ends, the sender's side and the receiver's side, such distribution of matrices can be performed exactly in the same manner, just agreeing a few analytical mathematical functions or according to the above exemplary embodiments positions of digits to be taken sequentially for achieving a distribution control scheme according to Figure 5d. The used arguments for the analytical mathematical functions may be transmitted before forming the distribution matrices A and B. They may also be contained in custom made encryption or decryption chips and therefore not known to the user. As a further embodiment they may also be transmitted via the data link, before encryption takes place,

e.g. encrypted according to a standard encryption method not necessarily having high safety requirements, since the key words to be transmitted are only short.

An example of how the invention works is shown in **Figure 6** and Figure 7. A difficult encrypting problem is a matrix or a stream of characters which are all the same for a lengthy period. This lengthy period is for example 50 lines of "e" in Figure 6 and this is encrypted according to two 10x10 matrices in Figure 3a and Figure 3b and with the help of the key values mentioned in item 1 earlier along this description, where the user key data was described. Figure 7 has virtually no remaining correspondence if compared to a stream of "e", there is no cycle determinable and the encrypted data looks like a complicated text or graphical representation, no ressemblance of a stream of only "e" appears. From Figure 7, it can be taken that two indexes were used. The amount of characters is twice after being encrypted.

The method according to the invention may be attacked from three sides:

1. The attacker attempts to find out the user inputs (keys):

   a) Systematically:

      Practically, $10^4 + 96^{30}$ possibilities (that means 2.7E+59 combinations) and theoretically, $10^4 + 224^{30}$ possibilities (which means 3.2E+70 combinations) must be tried.

   b) By selected sampling:

      With clever selection of the inputs and the multi plicity of chances this would mean: To find the famous needle in the haystack (possible but un likely).

2. The attacker knows the principle of the method and he is

trying to find the matrix system and the transformation factors.

a) Finding the matrix system is depending on the number system applied and the characters used in the matrix. The characters used are defined in the program. They can be defined differently in every program. If the plaintext is only encrypted once the following values will ensue from the quantity of characters contained in the respective matrix:

Upper limit

Matrix	Sum of characters	4-digit number	Combinations
(10x10)	100	9,999	3.6E+6
(11x11)	121	14,640	3.9E+7
(12x12)	144	20,735	4.8E+8
(13x13)	169	28,560	6.2E+9
(14x14)	196	38,415	8.7E+10
(15x15)	225	50,624	1.3E+12
(16x16)	256	65,535	2.1E+13
(17x17)	289	83,520	3.5E+14
(18x18)	324	104,975	6.4E+15
(19x19)	361	130,320	1.2E+17
(20x20)	400	159,999	2.4E+18
(26x26)	676	456,975	4.0E+26
(30x30)	900	809,999	2.6E+32
(36x36)	1,369	1,679,615	3.7E+41
(40x40)	1,600	2,559,999	8.1E+47
(50x50)	2,500	6,249,999	3.0E+64
(64x64)	4,096	16,777,216	1.2E+89

In case of multiple encryption, including different key data, the probability of a systematic attack leading to a deciphering of the ciphertext is virtually near impossible.

b) Transformation

Transformation to a 4-digit number of the respective number system includes variations ranging from the initial number to the 4-digit number itself (addition, subtraction, multiplication, division, shifting of bits). In addition, transformation is also depending

on user inputs (key data) which will influence the determination of the 4-digit number.

3. Trying to find the plaintext from the distribution and the frequency of the encrypted characters (ratio of plain characters and encrypted characters). The cipher characters are depending on the following determination factors:

(1) On the matrix, generated in the program from the available characters (type and amount) and

(2) on the 4-digit number in the respective number system (i. e., on the transformation and thus on the user inputs). As examples for the ratio (variability), 10 lines of letter "e" in plaintext (840 characters) result in the following distributions in the encrypted text, using the key words as given in case 1, case 2, case 3.

Case 1: [ ], [ ], [ ]

Case 2: [1234], [9876-543-ABC], [Mount Everest]

Case 3: [4711], [dtbank375481220], [popocatepetl]

	Different characters	Double characters	Variability (sum/double)
Matrix 10x10			
Case 1	724	76	10.52
Case 2	755	45	17.77
Case 3	730	70	11.42
Matrix 15x15			
Case 1	743	57	14.03
Case 2	770	30	26.22
Case 3	744	56	14.28
Matrix 20x20			
Case 1	746	54	14.81
Case 2	775	25	32.00
Case 3	747	53	15.09
Matrix 50 x 50			
Case 1	748	52	15.32
Case 2	775	25	32.00
Case 3	748	52	15.38

* * *

Claims:

1. **Method** for the encryption of input data, especially when transmitting an encrypted file within electronic networks, comprising the steps of
   (a) providing at least one field input in a coding step to define at least a first array or matrix with distributed ASCII elements, which ASCII elements are filling said matrix or array purposeful and unique, but in a distributed manner;
   (b) said input data is transformed via a transformation to at least a first and a second index, uniquely addressing said at least one array or matrix in order to determine encrypted characters.

2. Method according to claim 1, wherein the dimension of said distribution arrays or matrices is between one and nine.

3. Method according to claim 1, wherein the transformation has a cycle of a modulo-behaviour.

4. Method according to claim 1, adapted to operate ASCII-oriented.

5. Method according to one of the above claims, wherein three field inputs are provided.

6. Method of decoding a file which was encoded according to claim 1, whereby said at least one field input at the receiving end controls the filling of said at least one distribution array or matrix in an identical manner as had been done at the encoding sender's side, on the basis of which at least one matrix the encrypted data is reconstructed via the recovered index of the at least one matrix and the inverse transformation as original input data.

7. Method according to claim 1, in which the encrypted characters are collected in an encrypted file for transmission purpose, to start after said encryption has converted a full input data file to a full transmittal encrypted file.

8. Method according to claim 1, the encryption proceeding substantially at the input rate of the input characters and the transmittal taking place at approximately the same speed.

9. Method according to claim 1, wherein the data input are one of:
- characters of plaintext,
- binary data of files,
- at least a part of a pixel information of a picture,
- an already encoded file using a data compressing or
- basic data encryption method.

10. Method according to claim 9, wherein the picture is a video picture comprising at least one of JPEG, MPEG and one of the standard picture formats.

11. Method according to claim 1, wherein more than one, preferably two arrays or matrices are employed, wherein each matrix or array is uniquely addressed by the transformed input data and each output of each array is combined to form the encrypted character.

12. **Method** for the encryption of text file input for transmittal via a data link comprising at least one sender and at least one receiver, characterized by a method according to one of the aforementioned claims.

13. Method according to claim 1, wherein the transformation is based on a long irregular but at both ends of the transmittal reproducible sequence of digits, a selected digit of said sequence used for one encryption step before proceeding to a next selected digit and succeeding encryption step.

14. Method according to claim 1, wherein said at least one field input provides
(a) an irregular but reproducible sequence of characters (predetermined digit sequence) used step by step to transform the input data to said indexes for said at least one array; preferably
(b) a digit sequence of a length corresponding with the places of at least one of said arrays, in said sequence no digit appearing twice.

15. Method according to claim 13 or 14, the sequence at both ends being independently reproducible, based on prior knowledge of agreed mathematical functions or places of digits in a long sequence of digits.

16. Method according to claim 15, wherein the arguments of said functions are derived from prior transmitted field inputs.

17. **Device** in chip form for executing the method according to claim 1 or claim 12, comprising
a sequential and combinational logic with at least one storage area for accepting and storing ASCII elements to logically form at least one array;
a distribution control section to place said ASCII elements in said at least one storage area in a sequence or organisation which is departing from their regular and standard sequence, to form a logically organized array with non-regular distributed ASCII elements;
an index generating unit to generate index data for addressing said at least one storage area, said unit being operable to provide said index data according to a given rule and one of: manual field input, transmitted field input and built-in field input.

18. Device according to claim 17, wherein
an input data conversion unit is operable to supply input data step by step to the index generating unit, to form indexes to address said at least one array in said storage area to select one of said distributed ASCII characters;
an output driver unit is provided, to be operable to accept said selected ASCII element and transmit it as encrypted character via a data link or store it in a file of encrypted characters.

19. Device in chip form adapted to work in reverse order than the device according to claim 17, with respect to reverse addressing of said at least one array in said at least one storage area.

20. Device according to claim 19, having an input receiver unit, to be operable to accept encrypted data and pass it via a data bus system to a selection unit, determining the indices of such encrypted data from said array, comprising said non-regular distributed ASCII elements.

* * *

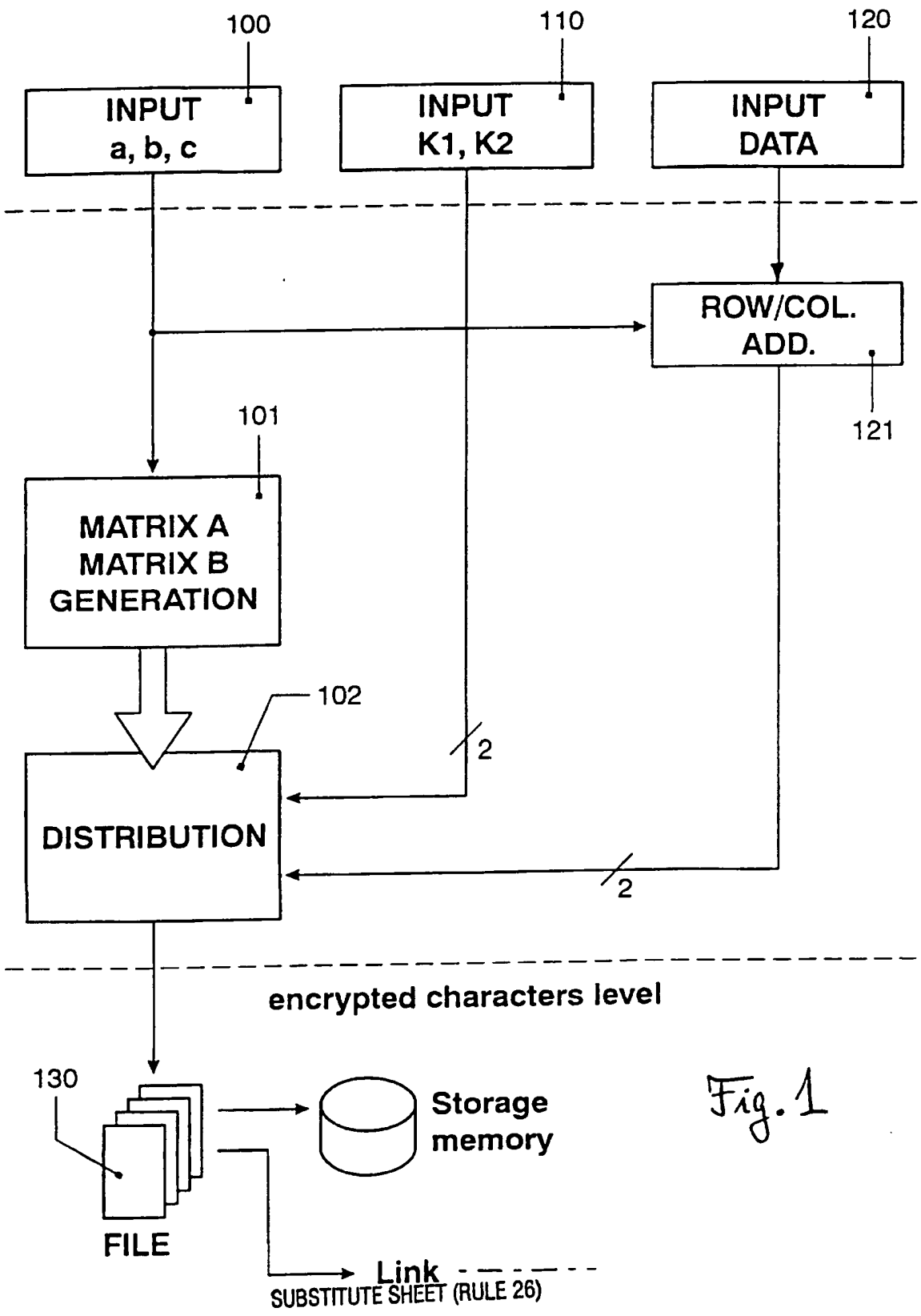

readable characters level
100
110
120
INPUT a, b, c
INPUT K1, K2
INPUT DATA
ROW/COL. ADD.
121
101
MATRIX A MATRIX B GENERATION
102
2
DISTRIBUTION
2
encrypted characters level
130
Storage memory
FILE
Link

Fig. 1

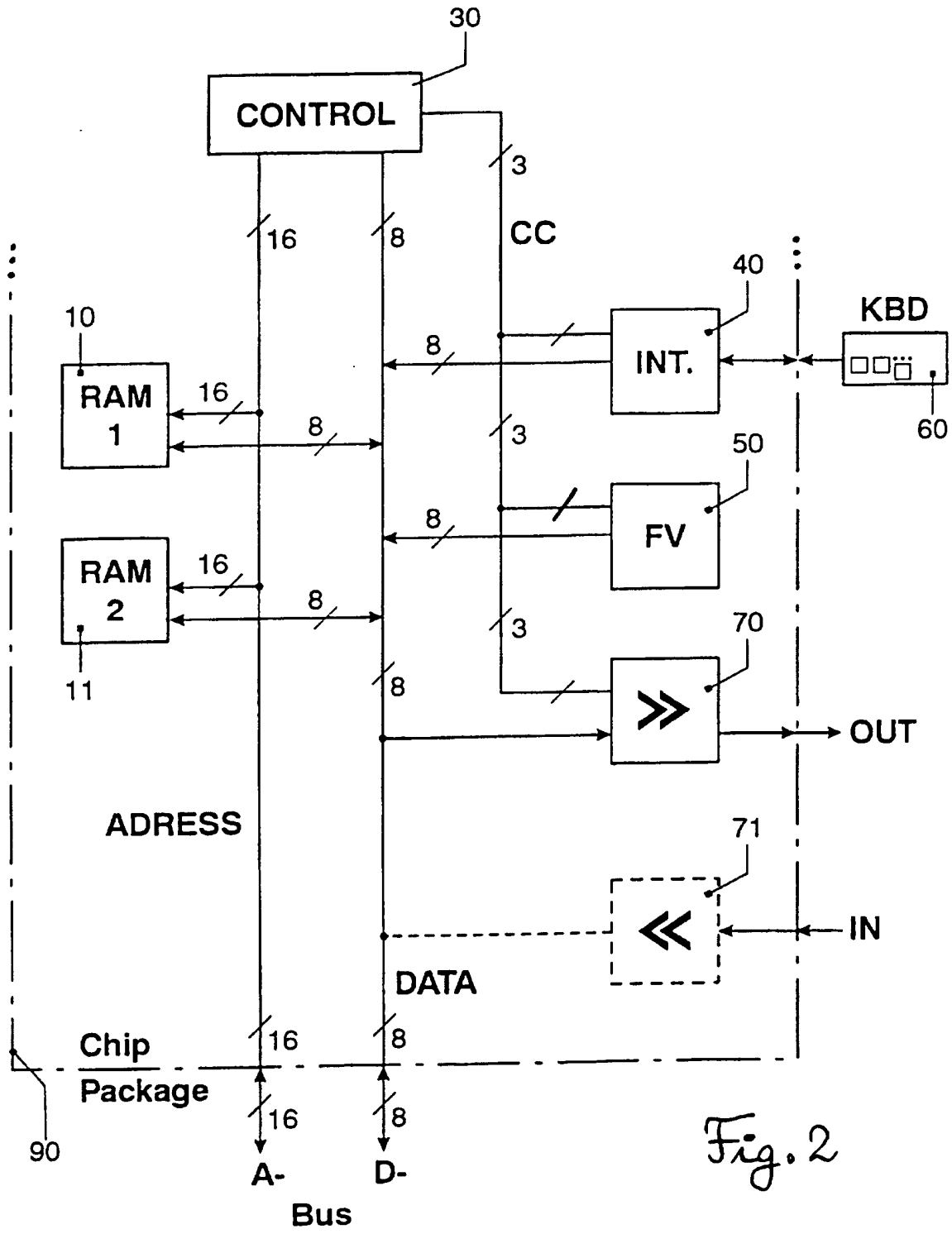

30
CONTROL
3
CC
16
8
40
KBD
10
INT.
8
RAM
1
16
8
3
60
50
FV
8
RAM
2
16
8
3
70
11
8
OUT
ADRESS
71
IN
DATA
Chip
Package
16
8
90
16
8
A-
D-
Bus

Fig. 2

Figur 3a
Matrix A (10x10)

<	ë	\	t	U	c	Ç	G	|	Õ
W	p	V	i	ü	D	y	Ü	?	î
}	ò	:	ì	^	q	P	a	ä	L
{	û	9	Ä	`	s	O	b	â	J
ê	K	w	ö	=	É	]	n	M	f
X	o	T	g	é	C	z	£	A	ï
å	I	x	ô	>	Æ	_	m	N	e
;	è	[	r	S	d	Ô	H	~	¢
Q	h	à	F	u	ÿ	B	æ	Y	l
R	j	ç	E	v	ù	@	Å	Z	k

Figur 3b
Matrix B (10x10)

-	H	n	l	y	I	w	,	B	C
z	a	å	ç	<	`	:	{	Y	[
M	G	+	*	h	E	i	L	v	x
e	Z	~	Δ	à	X	ä	c	7	6
F	r	O	Q	.	s	/	D	f	g
T	5	b	d	ü	4	â	U	ë	ê
q	j	A	@	N	k	P	p	3	1
8	ï	R	S	_	ì	^	9	é	Ç
m	0	u	t	>	2	?	o	J	K
è	}	=	;	W	|	V	î	]	\

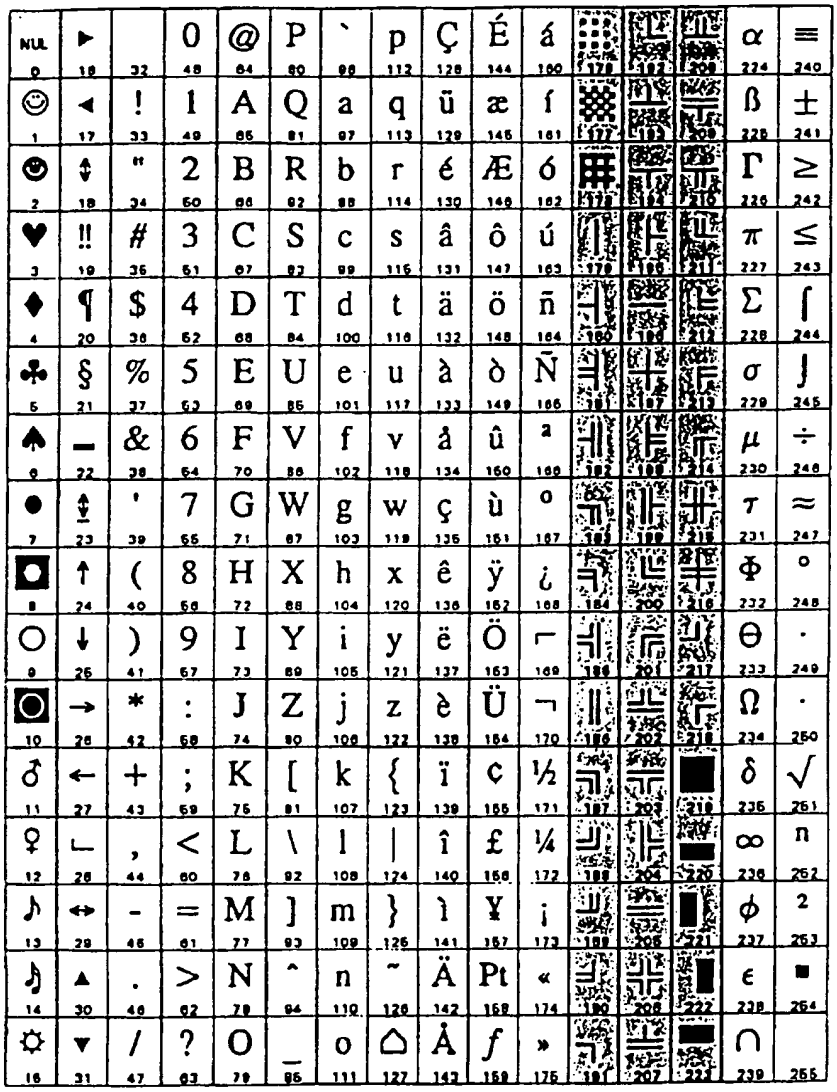
Figur 4a
MATRIX A (15x15)

"	è	╫	z	v	┐	ù	Y	╠	f	C	°	3	δ	Ñ
.	∩	«	*	Ä	┌	~	s	┤	Ü	N	╚	\	I	√
n	╣	ú	V	-	h	E	n	4	θ	½	(	Ç	╥	{
ß	┌	!	î	┴	à	t	┤	ñ	T	╧	a	D	÷	7
F	}	k	┴	¿	L	╤	c	H	≈	5	ᴛ	»	^	ï
·	-	σ	<	■	ë	■	â	j	┬	ƒ	W	╩	b	B
S	╓	d	■	1	0	μ	°	+	Æ	╦	å	r	└	¥
╩	e	=	╛	┘	ϕ	¼	&	ì	■	x	m	╗	¢	M
`	F	≡	Ω	¬	¬	┘	ö	▌	Y	w	╩	Ô	R	╤
—	·	ô	═	o	o	Å	û	é	╞	_	>	²	8	Γ
G	±	;	£	%	┬	≤	╪	π	ì	╕	Ö	P	┼	g
╗	Pt	Q	[	@	·	^	2	┘	▓	)	ê	α	ü	u
ä	p	╝	q	┼	á	9	?	¡	/	є	▒	-	Ò	▌
ÿ	X	╬	╖	╢	┴	K	Φ	]	$	æ	╥	—	1	╣
É	▌	╬	q	J	á	K	╫	j	A	≥	:	∞	▪	,

Figur 4b
MATRIX B (15x15)

	'	]	■	╙	°	Q	°	Δ	^	E	▒	E	Ä	Ä
ê	ϕ	┼	°	{	+	╬	+	D	∈	∩	%	9	■	■
F	¼	í	ē	i	π	b	C	ϵ	/	9	æ	Φ	}	}
x	(	T	╤	┐	•	:	;	Γ	Γ	Φ	╫	»	o	o
t	î	┬	â	ƒ	!	≥	n	¿	¿	#	˜	#	┐	┐
╝	╪	f	r	J	ç	.	4	^	^	ì	m	ì	Pt	Pt
ò	—	C	—	±	▌	Σ	δ	Æ	Æ	╥	╝	╥	I	I
W	q	·	ó	a	ü	Ñ	┌	▌	▌	Ç	ö	Ç	┼	┼
╧	▓	2	R	F	h	)	$	w	w	g	M	g	⌊	⌊
d	ÿ	ᴛ	═	⌡	L	É	ï	u	u	╬	-	╬	?	?
A	L	⌐	╤	3	¥	╤	r	╗	╗	ù	]	ù	≡	≡
÷	╞	&	B	σ	U	ä	Γ	á	á	N	<	N	8	8
1	Z	à	⌠	¡	╙	p	v	P	P	┼	√	┼	Ω	Ω
θ	G	┡	5	\	`	┘	k	╒	╒	e	6	e	ñ	ñ
ú	·	y	ë	ë	@	¢	╪	╒	╒	╞	α	╞	*	*

Figur 4c


NUL 0 ▶ 16 32 0 48 @ 64 P 80 ` 96 p 112 Ç 128 É 144 á 160 α 224 ≡ 240
☺ 1 ◀ 17 ! 33 1 49 A 65 Q 81 a 97 q 113 ü 129 æ 145 í 161 ß 225 ± 241
☻ 2 ↕ 18 " 34 2 50 B 66 R 82 b 98 r 114 é 130 Æ 146 ó 162 Γ 226 ≥ 242
♥ 3 ‼ 19 # 35 3 51 C 67 S 83 c 99 s 115 â 131 ô 147 ú 163 π 227 ≤ 243
♦ 4 ¶ 20 $ 36 4 52 D 68 T 84 d 100 t 116 ä 132 ö 148 ñ 164 Σ 228 ⌠ 244
♣ 5 § 21 % 37 5 53 E 69 U 85 e 101 u 117 à 133 ò 149 Ñ 165 σ 229 ⌡ 245
♠ 8 ▬ 22 & 38 6 54 F 70 V 86 f 102 v 118 å 134 û 150 ª 166 μ 230 ÷ 246
● 7 ↨ 23 ' 39 7 55 G 71 W 87 g 103 w 119 ç 135 ù 151 º 167 τ 231 ≈ 247
◘ 8 ↑ 24 (40 8 56 H 72 X 88 h 104 x 120 ê 136 ÿ 152 ¿ 168 Φ 232 ° 248
○ 9 ↓ 25) 41 9 57 I 73 Y 89 i 105 y 121 ë 137 Ö 153 ⌐ 169 Θ 233 · 249
◙ 10 → 26 * 42 : 58 J 74 Z 90 j 106 z 122 è 138 Ü 154 ¬ 170 Ω 234 · 250
♂ 11 ← 27 + 43 ; 59 K 75 [91 k 107 { 123 ï 139 ¢ 155 ½ 171 δ 235 √ 251
♀ 12 ∟ 28 , 44 < 60 L 76 \ 92 l 108 | 124 î 140 £ 156 ¼ 172 ∞ 236 n 252
♪ 13 ↔ 29 - 45 = 61 M 77] 93 m 109 } 125 ì 141 ¥ 157 ¡ 173 ϕ 237 2 253
♫ 14 ▲ 30 . 46 > 62 N 78 ^ 94 n 110 ~ 126 Ä 142 Pt 158 « 174 ε 238 ■ 254
☼ 15 ▼ 31 / 47 ? 63 O 79 _ 95 o 111 ⌂ 127 Å 143 f 159 » 175 ∩ 239 255

Figur 5a

Matrix A

Ö ä O j ô û å N e æ
K ? \ w t M < ^ v o
Q i Å ÿ ü V k Î Ü Ç
X y s I > Y ~ u F @
É ö â U g Ä ò ê W d
n J : { } q H ; ` Ô
ë P h è ù ç S f ï £
B a x r D = _ { p E
c Æ ¥ é T b Ï ç ã R
z m L C Z | 1 G A]

Figur 5c

1369446624823060233464894831417944126354444639890645796558744579655874457965587445796558744579655874
2741893060648926858604035518959767338681178709354417870935446506697567324692797827418930606489268586040355189597673386811787093544178709354465066975673246927978

Figur 5d

1	3	6	9	4	5	7	8	2	0
2	7	4	1	8	9	3	0	6	5

Matrix B

è u @ [ä ç w ? V é
< 0 M h e > - O g `
B Z Ç ë r G \ } ï q
I j d : / J o f 7 1
ü à t F X Ô å y H U
_ ; + L n b 9 , Q p
z A Y { ê x D W | î
3 R i c 5 . P l a 6
T â Ä s E S ~ î v C
k ^ = 4 K m] 8 2 N

Figur 5b

Figur 6

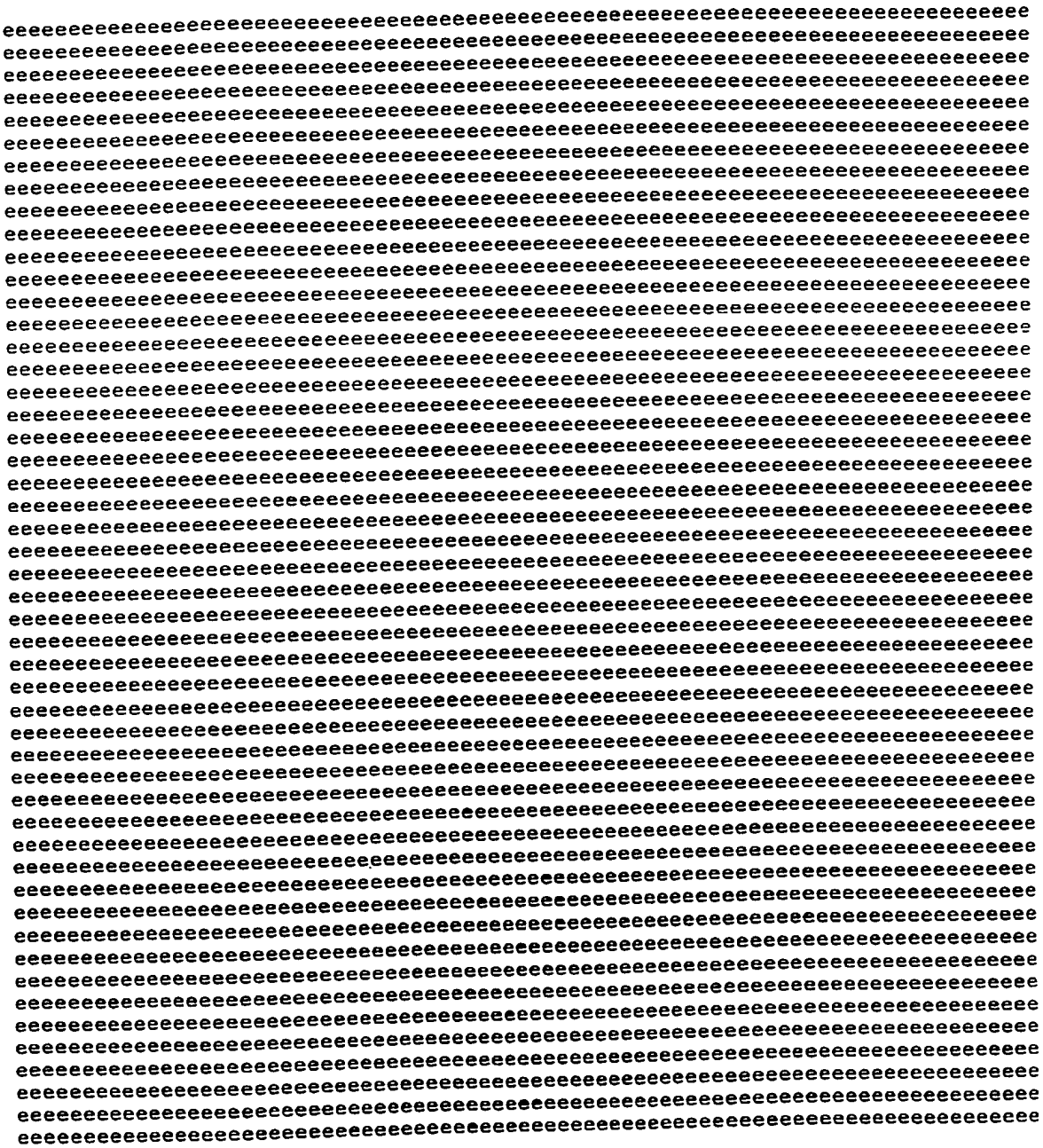


Fig. 7 (Part 1)

Continued ...

Figur 7
(Part 2)

\ã~Js0\?ühgUsZew<0eVÉjüIQgg,sqsX<~ÛåQrsHsJüùÉFQfû:ÜUQdÉDûfÜL~H~xüã~W\/QUs;sDÜ_\F
ûU~.ü;~lQ_gCÉWÜReOû|ûp~S~3~îsîgNÜ|Ûã~PûaûîÜS~Ts=s6ÃéÜaÜ^~~u[û6<T~kI@sC<EÜvÄZ~]</
\Tu>s8\îü4ÃqIue~<^evõ0V<Q2ÂfI6Ir<NÇZ1äIîI>VBõêiOVhÇqiMõåVOÇ:uîuΩVZuyweiqIjIåÇIwë
VqubVju,iIÃîöyÇ;æGVHV1uxu_uWIUÃ6ÇHÇAu9VQVUÇxuzIiIpÄCÇQÇRuDusVp^zu3IÄIî^êÇ|ôuuP^e
wzumIlwWVcõéIâæD^Ræ|õ~VkiaõOIC>å~6XuiE>VImkêâ[i8V4X6i=ã\V8XhFVPGkuF}wKÅé>0>\X<t[
kéPJk0PfÅ<õUâ}XjKçkik~FΩFIPy>qõpXîXãFok7kqXΩFü>+>lõîX7X;FåP{klvüP_>Y>UvXXHõãF9^K
tüF.>,tykLõC>AKåv;KHãRk3ÅQâmXWXÂt,k6vYX~XcÅaFâv.ÅRkîv3@ãÅ.k^>~Y[Å6YçKivÎXCyäkvKâ
ÂîYhÅCY>vvU)@çÎéåsÿwÅ8YëYVYGy?Ufîwî~Yeÿ-ÿ?îëYgyIyOUyî-îqYrYäÿOMgYiyüy}MÇÎ\UpY/ti
?gYLyJ?GÿjUWylNrMqN\@UÿHooU.yyyYMfîpotyDyLÿQ@Aobÿ;îWo_@EÿbîRYDYsÿpYS?+oWyIyEî|?A
ÿWY4ÿîYmo|g?@SîCN{ÿ~ÿl~[Yv~çyîgOî~îNYKÿ}ÿîÛ[Y2s<y8g}î]Ü6~ã~Zÿ8M2~VsBs?<@Üwgl~eM+
?2~:s>\çü0gys~eä<éewÉqüîQ-gbs}st<OÜ1QÇsås:ü7ÉàQJüjÜyQIÊêüJÜ;~å~{ül~x\dQysUsêÜH\à
üy~cüU~.QHgîÉxÜîePüDü,~s~|~SsWg8ÜDÜ6~5üPûWÜs~askslÃ?ÜPÜC~Euuül<a~vIèsî<ÃÜ~Ã~~K<d
\auhsm\Sü^Ã}sNeE<Ce~õ6VVQ]ÄJI7IÇ<8Ç^i@I\IhVgöZi>V0Ç}i<öXV>Çju\uFV~uΩwMi}IqIXÇiwZ
V)uLVqubiîÄWöOÇUæëVåVfu{uHuxIyÃlÇåÇpunV9VyÇ{uQI3I,ÂîÇ9ÇîuêuõV,^Qu|ITIW^YÇDÃNu5^M
wQu4I.wxVRõ?I6æê^îæDõCVviPõ>Iî>@^lÇNiÃ>wI4V2âuimV^X?ikârVmX0FwFëVNFGw=Å?>é>rXVtu
k?P:kéFJÅVõyâGXqK[k\kOFFFîFΩ>}õ,X\X1F/kok}XFF7>_>fõWXoXUFXFAkfv7FH>z>yvtXåõ6Fn^=
t7Fc>btΩk;öî>pKXvUKåãik|Å9òm>WXTtbklvzXEXRÅPF6vcÅîkSv|@@ÅckC>EYuÅlY[K3vSXîy@k~K6
ÅSY0ÅîYhv~UG@[î?âåÿäÅmYZYwYëyçUJîäîOYMÿeÿçîZY-yîy>UΩîeî}YÇY1ÿ>M-Y\y7yGMBîrU,Ydt3
?-Y;y:?éÿqUxyfNÇM}Nr@yÿåo/UcyΩyzMJî,oüyêy;ÿ9@poLÿUîxoH@ÃÿLîîYêYâÿ,Ys?_oxyWyÃîD?p
ÿxY^ÿWY4oDgç@sîîNAÿEÿ.~uY~~[ySg>îEî8Y=ÿKÿSÜuY]sVymgGîKÜ?~@~~ÿmM]~wsgsç<êÜägf~MM_
?]~jsh\[üégΩsOe@<?eãÊ}ü\QegLsGsü<>ÜfQBsXsjüoÉ1Q:üqÜΩQîÉYü:ÜU~X~Aüf~{\IQΩsysYÜå\1
üΩ~Rüy~cQågSÉ{ÜWeâûêüb~â~D~ssxgmÜêÜl~iü5üxÜâ~Psvs.ÄçÜ5ÜîîÃ~Nü.<P~~s2sS<TÜEÃO~=<I
\Pu0s4\süCÄGs8eÃ<îeEõ?VwQKÃ:IçIB<mÇOiêIrI0V-õ^ihVéÇGiVõtVhÇquruäVOuFw<iGI}ItÇ\w^
VGu;V}uLi\ÃxöFÇyæZVXVJuAuåu{IΩÃ.ÇXÇ,u+VnVΩÇAu9I|IbÅSÇnÇWuYu6Vb^9uDIaIx^zÇêÄ8ui^<
w9u^Icw{ViòçIlæY^WæêõîV~i5ðhIS>ê^.Ç8iT>äI^V]öNi4VCXçivâÇV4XéPäPZV8PëwkÅç>?>ÇXwwN
kçPjk?P:ÅwöΩêëX}Kukrk>FäF\FP>GõbXrXfFdk/kGXãFo>H>JõxX/XyFtFpkJvoFå>Q>ΩvüXXõlF+^k
toFR>LtFkUõS>,KtvyKXãWkDÅnõ4>x>Tvbk.vQXÃXiÅ5FlvRÅWksvD@êÅRkî>Ã>NÅ.YuK|vsXSyêkEKl
ÅsY6ÅSY0vEUë@uîçå6ÿ@Å4Y~YäYZy[U:f@î>Y<ÿMÿ[î~Yey\yhUFîMîGYBYfÿhMeYryoyëMgîÇUbYIt|
?eYUyj?Zÿ}U{yJNBMGNÇ@ΩÿXodURyFyQM:îbo7yYyUÿn@,o;ÿyî{oå@Tÿ;îWYYY6ÿbYâ?Ho{yxyTîê?,
ÿ{YCÿxY^oêg[@âîSNpÿÄÿcYNYE~uysghîÃîmYkÿ=ÿsîNYKswy4gëî=Üç~ê~Oÿ4MK~äs-s[M2Ü@gJ~<MH
?K~qs0\uü?gFs>eê<çe@ÉGürQMg;sës7<hÜJQgstsqü/ÉfQjü}ÜFQ\ÉzüjÜy~t~püJ~A\îQFsΩszÜX\f
üF~iüΩ~RQXgsÉAUxe1üYüL~6~ê~âs{g4ÜYÜ.~3üiü{Ü6~5s~scÃ[ÜiÜS~T~8üc<5~Es]ss<aÜÃÃ>~k<i
\5ués^\åüîÃësmeT<SeÃõçVãQ=ÃjI[Ig<4Ç>Q2IÇIéVeõOi0V?Çêiwõ üVOÇ}uÇulV>uàwViêIGIüÇrwO
VêuUVGu;irÃ{õãÇΩæ~VtV:upuXuAIFÃcÇtÇbu_V+VFÇpunIDILÃsÇ+ÇxuzulVL^nuêIPI{^QÇYÃmu3^V
wnuCIRwAVWõ[I.æz^xæYõSVEiiõ0IsI2^cÇmia>@ICVKõ8i~VîX[i~ãBV^X?F@F~VmFZwvÅ[>ç>BXãw8
k[FqkçFjÅãõFãZXGmNkÇkhFlFrFà>ëõLXÇXJFIkdkêX1F/>å>:ò{XdXΩFüP,k:v/FX>9>Fv7Xtõ.F_~v
t/Fî>;tãkyõs>bKüvΩKtãxkêÅ+õ^>{>avLX.ÅQXTXWÅiF.viÅxkãvêF2ÅîkS>T>8Åc>NKDvâXsX2kÃK.
ÅãY?ÅsYévÃUZFNî[ålÿèÅ^YOY@Y~yuUjîêîhYVÿ<ÿufOYMyry0Uãî<îëYgYJÿ0MMYÇy/yZM-îBULYîtD

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/EP 97/04062

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 363 449 A (BESTOCK RALPH R) 8 November 1994 see column 4, line 6 - line 20 see column 5, line 16 - line 42	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
21 November 1997	04/12/1997

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Larcinese, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l Application No
PCT/EP 97/04062

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5363449 A	08-11-94	CA 2118644 A	12-09-94